(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 January 2003 (09.01.2003)

PCT

(10) International Publication Number
WO 03/003687 A1

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/IB02/02589

(22) International Filing Date: 28 June 2002 (28.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/894,391 28 June 2001 (28.06.2001) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: EPSTEIN, Michael; Prof . Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

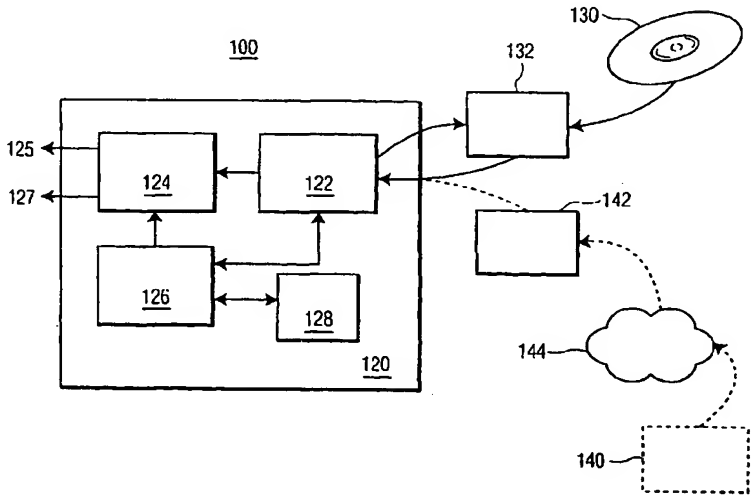
(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TEMPORAL PROXIMITY TO VERIFY PHYSICAL PROXIMITY



(57) Abstract: A security system (100) assesses the response time to requests for information to determine whether the responding system (132, 142) is in physical proximity to the requesting system. Generally, physical proximity corresponds to temporal proximity. If the response time indicates a substantial or abnormal lag between request and response, the system assumes that the lag is caused by the request and response having to travel a substantial or abnormal physical distance, or caused by the request being processed to generate a response, rather than being answered by an existing response in the physical possession of a user. If a substantial or abnormal lag is detected, for example due to the fact that the information was downloaded from the Internet (140, 144), the system (100) is configured to limit subsequent access to protected material by the current user, and/or to notify security personnel of the abnormal response lag.

WO 03/003687 A1

Temporal proximity to verify physical proximity

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of data protection, and in particular to protecting data from illicit copying from a remote location.

2. Description of Related Art

The protection of data is becoming an increasingly important area of security. In many situations, the authority to copy or otherwise process information is correlated to the physical proximity of the information to the device that is effecting the copying or other processing. For example, audio and video performances are recorded on CDs, DVDs, and the like. If a person purchases a CD or DVD, the person traditionally has a right to copy or otherwise process the material, for backup purposes, to facilitate use, and so on. When the person who purchased the material desires to use the material, it is not unreasonable to assume that the person will have the CD or DVD within physical proximity of the device that will use the material. If, on the other hand, the person does not have proper ownership of the material, it is likely that the person will not have physical possession of the material, and hence, the material will be physically remote from the device that is intended to use the material. For example, the illicit copying or rendering of material from an Internet site or other remote location corresponds to material being physically remote from the device that is used to copy the material.

In like manner, security systems are often configured to verify information associated with a user, such as verifying biometric parameters, such as fingerprints, pupil scans, and the like. In a simpler example, security systems are often configured to process information provided by a user, such as information contained on an identification tag, smartcard, etc. Generally, the information or parameters can be provided easily by an authorized user, because the authorized user is in possession of the media that contains the information. An unauthorized user, on the other hand will often not have the original media that contains the verification information, but may have a system that can generate/regenerate the security information or parameters from a remote location.

Similarly, some systems, such as an office LAN, or computers in a laboratory, are configured to be secured by controlling physical access to terminals that are used to access the system. If the user has access to the system, the assumption is that the user is authorized to access the system. Some security measures, such as identification verification, are sometimes employed, but typically not as extensively as the security measures for systems that lack physical isolation.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to provide a system or method of preventing the use of material in the absence of evidence that the material is in the physical possession of the user. It is a further object of this invention to prevent the use of material in the presence of evidence that the material is remote from the device that is intended to use the material. It is a further object of this invention to prevent access to systems in the presence of evidence that the user is remote from the system.

These objects and others are achieved by providing a security system that assesses the response time to requests for information. Generally, physical proximity corresponds to temporal proximity. If the response time indicates a substantial or abnormal lag between request and response, the system assumes that the lag is caused by the request and response having to travel a substantial or abnormal physical distance, or caused by the request being processed to generate a response, rather than being answered by an existing response in the physical possession of a user. If a substantial or abnormal lag is detected, the system is configured to limit subsequent access to protected material by the current user, and/or to notify security personnel of the abnormal response lag.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawing wherein:

FIG. 1 illustrates an example control access system in accordance with this invention.

Throughout the drawing, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

For ease of reference and understanding, the invention is presented herein in the context of a copy-protection scheme, wherein the processing of copy-protected material is controlled via a verification that the user of the material is in physical possession of the copy-protected material.

FIG. 1 illustrates an example control access system 100 in accordance with this invention. The control access system 100 includes a processor 120 that is configured to process material from a physical media, such as a CD 130, via an access device 132, such as a reader. The storage medium 125 such as a processor 120 may be a recording device that records one or more songs from the CD 130 onto a memory stick, onto a compilation CD, and so on. The processor 120 may also be a playback device that is configured to provide an output suitable for human perception, such as images on a screen, sounds from a speaker 127, and so on. The term "rendering" is used herein to include a processing, transformation, storage, and so on, of material received by the processor 120. Using this context and terminology, the example processor 120 includes a renderer 122 that provides the interface with the access device 132, and a verifier 126 that is configured to verify the presence of authorized material 130.

When a user commences the rendering of material from the media 130, the processor 120 is configured to verify the presence of the media 130. One method of effecting this verification is to request the access device 132 to provide evidence that the media 130 is available to provide material or information that differs from the material that the user is attempting to render. For example, if the user commences the rendering of a song, the verifier 126 may direct the renderer 122 to request a portion of a different song from the access device 132. If the access device is unable to provide the requested portion of a different song, the verifier 126 can conclude that the media 130 is not actually present for rendering, and will terminate subsequent rendering of the material that the user intended to render, via the gate 124.

For example, a user may illicitly download a selection of different copy-protected songs from a remote site 140 on the Internet 144, and then attempt to create a compilation CD containing these user-selected songs. Typically, the size of an entire album of material discourages the downloading of each album that contains the user-selected songs. When the verifier 126 requests a portion of a different song from the album corresponding to an actual CD 130, the user who downloaded only the user-selected song from the album will be prevented from further rendering of the downloaded material.

A variety of techniques may be employed to assure that the material provided in response to the request corresponds to the material that is contained on the actual CD 130. For example, internationa patent application WO 01/59705 (Attorney Docket US000040) teaches a self-referential data set wherein each section of a data set, such as a copy-protected album, is uniquely identified by a section identifier that is securely associated with each section. To assure that a collection of sections are all from the same data set, an identifier of the data set is also securely encoded with each section. Using exhaustive or random sampling, the presence of the entirety of the data set is determined, either absolutely or with statistical certainty, by checking the section and data-set identifiers of selected sections.

The verification provided by the verifier 126 as described above can be defeated, however, by responding to the requests from the renderer 122 from the remote site 140 that contains the entirety of the album. That is, rather than downloading the entire album from the remote site 140, the illicit user need only download the desired song, and imitate the presence of the actual CD 130 by providing a CD imitator 142 that provides access to requested material or portions of material via the Internet 144. When the verifier 126 requests a portion of a song, or section of a data set, the CD imitator 142 transforms the request into a download request from the remote site 140, and the requested section is provided to the renderer 122, as if it was provided from the CD 130. Assuming that, for practical purposes, the verifier 126 will be configured to only check for a few sections in an album, the use of the CD imitator 142 will result in a substantially reduced amount of data transfer, compared to the downloading of the entire album, and thus preferable for the illicit download of select songs.

In accordance with this invention, the processor 120 includes a timer 128 that is configured to measure the time between a request from the verifier 126 and a response from an external source, either the actual CD 130, or the remote source 140, to facilitate an assessment by the verifier 126 of the physical proximity of the source of the response. In a preferred embodiment, the verifier 126 is configured to filter or average the response times, so as to allow for minor perturbations in the response time from an authorized source 130, while still being able to distinguish a response from a physically remote source 140. For example, using conventional statistical techniques, the verifier 126 may continue to request sections from the unknown source until a statistically significant difference from the expected response time of a local source 130 is detected. In a simpler embodiment, if the response time is below a delay threshold N out of M times, the verifier 126 is configured to conclude that the source must be local. These and other techniques for assessing physical proximity based

on temporal proximity will be evident to one of ordinary skill in the art in view of this disclosure.

The principles of this invention are applicable to other applications as well. In an analogous application, for example, the renderer 122 and access device 132 may be challenge-response devices that are configured to exchange security keys, using for example, a smart card as the media 130. If an unauthorized user attempts to exchange keys by processing the challenge-responses via access to a system that is potentially able to overcome the security of the exchange, the timer 128 will be able to detect the abnormal lag between the challenge and response, and terminate the key-exchange. In like manner, if a system expects all accesses to be from terminals that are in a common physically secured area, the timer 128 will be able to detect abnormal lags if the system becomes a target of a remote access 'hacker' or other attempted accesses from outside the physically secured area.

Preferably, the verifier 126 is configured to request random source information. In the example of a CD media 130, the verifier 126 is configured to request access to randomly selected sections on the media 130 until sufficient confidence is gained whether the source is local or remote. In other applications, the verifier 126 is configured to merely monitor, and time, transactions that routinely occur between a requesting device 122 and an access device 132, to detect abnormally long response times. In other applications, the verifier 126 may merely control the order of occurrence of routine data access requests. For example, when reading information from an user's identification device, the verifier 126 may be configured to sometimes ask for the user's name first, identification number next, fingerprint next, and so on; at a next session, the verifier 126 may ask for the identification number first, a voiceprint next, and so on, thereby preventing a pre-recorded sequence of responses.

Similarly, in an application intended to prevent the downloading of data from a remote site, the verifier 126 in the example of FIG. 1 may merely request portions of the requested data in a different order sequence, to determine whether the requested data is local or remote. In like manner, to prevent the unauthorized download of information from a network, the verifier and time may be placed at the remote site, and configured to measure the transport time of the data. For example, in a conventional network having error-detection capabilities, the verifier may be configured to purposely transmit erroneous data, or an erroneous sequence of data, and measure the time duration until a request-for-retransmission occurs. If the receiving site is local, the request-for-retransmission should occur substantially quicker than if the receiving site is remote. In this example, the erroneous transmission

constitutes a "requests" for a "response" from the receiving system. These and other timing schemes will be evident to one of ordinary skill in the art.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its scope. For example, although the invention is presented in the context of detecting responses that are abnormally slow, the principles of the invention can also be applied for detecting responses that are abnormally fast. For example, if a system is configured to read information from a magnetic strip on a card, there is an expected lag associated with the swiping of the card. If the information is provided without this lag, for example, from a computer that is configured to bypass the magnetic strip reader, a security alert may be warranted. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer

CLAIMS:

1. A security system comprising:

a verifier that is configured to determine an authorization to process protected material, based on one or more responses to one or more requests, and

a timer that is configured to measure response times associated with the one or more responses to the one or more requests;

wherein

the verifier is configured to determine the authorization based at least in part on an assessment of the response times.

2. The security system of claim 1, wherein

the verifier is configured to form the assessment based on at least one of:

an average of the response times,

a comparison of the response times to one or more threshold times, and

a statistical test based on the response times.

3. The security system of claim 1, wherein

the verifier is configured to provide the one or more requests, based on a random selection of one or more items to request.

4. The security system of claim 1, wherein

the response times are correlated to a physical proximity between a first source of the one or more requests and a second source of the one or more responses.

5. The security system of claim 1, wherein

the assessment of the response times forms an assessment of whether the one or more responses were communicated via a network connection.

6. The security system of claim 1, further comprising:

a renderer that is configured to receive a plurality of data items corresponding to a data set, and to produce therefrom a rendering corresponding to a select data item,

the verifier being operably coupled to the renderer, and configured to preclude the rendering corresponding to the select data item in dependence upon whether other data items of the plurality of data items are available to the renderer, and

the timer being operably coupled to the verifier and the renderer, and configured to measure response times associated with responses to requests for the other data items from the renderer.

7. A method for determining an authorization to process information based on a physical proximity between a receiver and a source of a plurality of data items, the method comprising:

determining a response time of the source of the plurality of data items, and

determining the authorization based on the response time.

8. The method of claim 7, wherein

determining the response time includes,

for each data item of a subset of the plurality of data items:

requesting the data item from the source at a first time,

receiving the data item at a receiver at a second time, and

accumulating a response time measure corresponding to a difference between the second time and the first time; and

determining the response time based on the response time measure.

9. The method of claim 8, wherein

the response time measure corresponds to at least one of:

an average of the differences between each second and first times,

a count based on a comparison of each difference to one or more threshold times, and

a statistical parameter based on the differences.

10. A computer program product arranged for causing a processor to execute the method of claim 7.

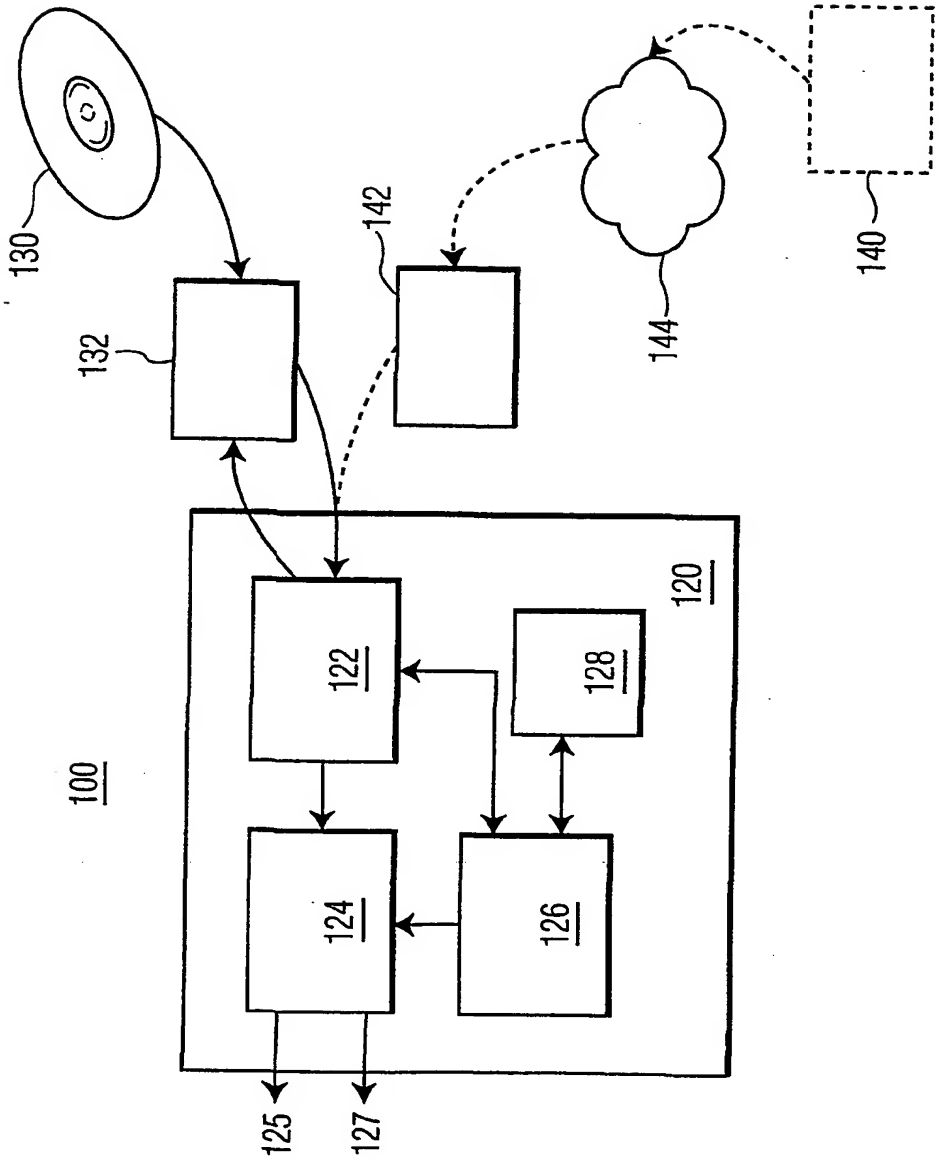


FIG. 1

INTERNATIONAL SEARCH REPORT

Int'l onal Application No
PCT/IB 02/02589

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 00 69111 A (RIENZO ANDREW L DI) 16 November 2000 (2000-11-16) page 19, line 20 -page 21, line 31	7,10 1,3-5
X	FR 2 781 076 A (VALEO SECURITE HABITACLE) 14 January 2000 (2000-01-14) page 1, line 4 - line 15 page 5, line 5 - line 27	1,2,4, 7-9
X	EP 0 983 916 A (MARQUARDT GMBH) 8 March 2000 (2000-03-08) abstract paragraph '0017! paragraph '0020! - paragraph '0021! paragraph '0026!	1,2,4, 7-9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 October 2002	23/10/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/IB 02/02589

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 029 259 A (SOLLISH BARUCH ET AL) 22 February 2000 (2000-02-22) column 5, line 9 - line 15 column 5, line 51 - line 66 column 6, line 45 - line 49	1,2
X	US 4 621 334 A (GARCIA JOHN D) 4 November 1986 (1986-11-04) column 1, line 5 - line 14 column 2, line 41 - line 58	1,2
A	US 5 659 619 A (ABEL JONATHAN S) 19 August 1997 (1997-08-19) column 1, line 7 - line 12 column 2, line 41 - line 49 column 5, line 23 -column 8, line 56	1,4,7
A	EP 1 073 244 A (IBM) 31 January 2001 (2001-01-31)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/IB 02/02589

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0069111	A	16-11-2000	AU	4831500 A	21-11-2000
			WO	0069111 A2	16-11-2000
FR 2781076	A	14-01-2000	FR	2781076 A1	14-01-2000
EP 0983916	A	08-03-2000	DE	19941428 A1	15-06-2000
			EP	0983916 A1	08-03-2000
US 6029259	A	22-02-2000	AU	4287999 A	05-01-2000
			CA	2335331 A1	23-12-1999
			EP	1086469 A1	28-03-2001
			WO	9966510 A1	23-12-1999
			JP	2002518784 T	25-06-2002
US 4621334	A	04-11-1986	NONE		
US 5659619	A	19-08-1997	AU	703379 B2	25-03-1999
			AU	2460395 A	05-12-1995
			AU	3675899 A	19-08-1999
			CA	2189126 A1	23-11-1995
			EP	0760197 A1	05-03-1997
			JP	11503882 T	30-03-1999
			WO	9531881 A1	23-11-1995
			US	6072877 A	06-06-2000
EP 1073244	A	31-01-2001	EP	1073244 A1	31-01-2001
			JP	2001077815 A	23-03-2001